DISA JIEO Standards Analysis **14 JUL 99**

Extended Key Usage Extension

References:

ITU-T Recommendation X.509, The Directory: Authentication Framework
RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile
TWG-99-01, Federal PKI X.509 Certificate and CRL Extensions Profile, section 1.2.4
MISPC, Minimum Interoperability Specification for PKI Components, Version 1, section 3.1.3.1
DOD Medium Assurance PKI Functional Specification (DRAFT) version 0.3 (20 OCT 98)

Implementation under analysis:

Analysis Date:

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
Key purposes may be defined by any organization. Are such organizational key purposes identified with OIDs assigned by IANA or according to ITU-T Rec. X.660 | ISO/IEC/ITU 9834-1? [X509: 12.2.2.4, RFC 2459: 4.2.1.13]		
Can this extension be flagged critical by the certificate issuer? [X509: 12.2.2.4]		
Does the application recognize the extended key usage extensions if it is flagged critical? [RFC 2459: 4.2]		
If the extension is critical, is the certificate used for only one of the purposes indicated? [X509: 12.2.2.4]		
Can this extension be flagged non-critical by the certificate issuer? [X509: 12.2.2.4]		
If the extension is non-critical, can the certificate be used for the purpose or purposes indicated? [X509: 12.2.2.4]		
If the extension is non-critical, then can it be used to find the correct key/certificate of an entity with multiple keys/certificates? [X509: 12.2.2.4]		
If the extension is non-critical, can the key be used for purposes other than that indicated? [X509: 12.2.2.4]		
Can the using applications require that a purpose be indicated in order for the certificate to be accepted? [X509: 12.2.2.4]		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
If a certificate contains both a critical key usage field and a critical extended key usage field, are both fields processed independently and is the certificate only used for a purpose consistent with both fields? [X509: 12.2.2.4]		
If there is no purpose consistent with both fields, is the certificate rejected? [X509: 12.2.2.4]		
Can the implementation support the key purpose of TLS Web server authentication (OID: 1.3.6.1.5.5.7.3.1)? [RFC 2459: 4.2.1.13]		
Can the implementation support the key purpose of TLS Web client authentication (OID: 1.3.6.1.5.5.7.3.2)? [RFC 2459: 4.2.1.13]		
Can the implementation support the key purpose of signing downloadable executable code (OID: 1.3.6.1.5.5.7.3.3)? [RFC 2459: 4.2.1.13]		
Can the implementation support the key purpose of e-mail protection (OID: 1.3.6.1.5.5.7.3.4)? [RFC 2459: 4.2.1.13]		
Can the implementation support the key purpose of time stamping (OID: 1.3.6.1.5.5.7.3.5)? [RFC 2459: 4.2.1.13]		
Does the DOD CA implementation never set this extension in any certificates issued? [DOD: Table 12, Table 13]		

Other information:

Findings:

Recommendations for Standards Work: